



# Bug 2424652 (CVE-2025-66286) - CVE-2025-66286 webkitgtk: Authorization bypass through WebPage::send-request signal handler

**Keywords:** Security ✕

**Reported:** 2025-12-23 17:47 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-04-23 12:21 UTC ([History](#))

**Alias:** CVE-2025-66286

**CC List:** 1 user ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability ☰ +

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**


**Whiteboard:**

**Depends On:** [2461113](#) [2461114](#) [2461115](#)  
[2461116](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport  2025-12-23 17:47:45 UTC	Description
	An API design flaw in WebKitGTK and WPE WebKit allows untrusted web content to unexpectedly perform IP connections, DNS lookups, and HTTP requests. Applications expect to use the WebPage::send-request signal handler to approve or reject all network requests. However, certain types of HTTP requests bypass this signal handler. Additionally, WebKit may create network connections that do not correspond to HTTP requests, such as for rel="preconnect". When WebKit is used by an email client, these flaws may be abused to allow the sender of an email to inappropriately detect that the email has been viewed by the recipient.

Affected versions: all versions of WebKitGTK and WPE WebKit

Credit to: Albrecht Dreß

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

